UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/485,352	03/13/2000	Michael DUPRE	2643/OG629	1819

7590 06/29/2005

Christa Hildebrand
NORRIS, McLAUGHLIN & MARCUS, P.A.
220 East 42nd Street
30th Floor
NEW YORK, NY 10017

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/485,352	DUPRE, MICHAEL	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: response filed on 13 December 2004, with an original application filing date of 14 March 2000 with a foreign priority date of 4 August 1997. Claims 14 and 19 are currently amended.

2. Claims 1-13 withdrawn from consideration indicated in pre-amendment, 4 February 2000.

3. Claims 14-26 are currently pending in this application. Claims 14 and 19 are independent claims.

Response to Arguments

4. Applicant's arguments with respect to claims 14-26 have been considered they are not persuasive where noted below. The arguments that are not noted below are moot in view of the new ground(s) of rejection.

As to applicant's argument beginning on page 5 "Thus, the claim expressly calls for all three parameters to be stored at the manufacturer of the chip ... In contrast, the storage of parameters (e.g., MSN, MSI) in the EPROM is not disclosed as occurring during manufacturing of the COB, as expressly called for in claim 19 ". The Office disagrees, the reference as a whole teaches the claimed invention see col. 7, line 40 through col. 8, line 67 of U.S. Patent 5,883,960 (hereinafter '960). Note '960 teaches that the COB device comprises a CPU 30, a RAM32, a ROM 34, and EPROM. Further '960 teaches that only the manufacturer of the mobile unit knows the KE_{MSNi}. Therefore it is inherent that the MSNi number is installed into the COB at time of manufacture.

As to applicant's argument beginning on page 7, 'Despite the Examiner's closing statement she has failed to expressly out where the '960 reference teaches the COB is Tool-kit enabled'. The Office disagrees the reference as a whole should be used as a basis for rejection the column and line numbers provided in the Office Actions are merely guides, see '960 col. 7, lines 41-59. This section shows what comprises the COB device and how the ROM contains a control program. The control program is interpreted as providing the same function as Tool Kit enabled.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 19-22, and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Maruyama et al. U.S. Patent No. 5,883,960 (hereinafter '960) in further view of Sudia U.S. Patent No. 5,799,086 (hereinafter '086).

As to independent claim 19, "A chip having a memory range, wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID), and an additional secret key Ki are stored" is taught in '960 col. 7, line 40 through col. 8, line 67 "FIG. 2 is a block diagram showing the configuration of the COB device 22 shown in FIG. 1. The COB device 22 comprises a CPU 30, a RAM 32, a ROM 34, and an EEPROM 36; the whole structure is sealed with resin, and only a power supply terminal

and an input/output terminal 38 for communication between the CPU 30 and the CPU 16 of the mobile unit are exposed. The structure is such that the contents of the internal EEPROM 36 cannot be read out or written in unless specific commands are input to the CPU 30 via the input/output terminal 38. The ROM 34 contains a control program 40 for the CPU 30, a password 42, and a common public key KE_{COB} 44 corresponding to a common secret key KD_{COB} determined through consultation among all communication carriers concerned ... KE_{COB} 44 is stored in order to enable a carrier public key KE_{Cj} (to be described later) which have been signature-encrypted with KD_{COB} to be decrypted and then to be written into the EEPROM 36. That is, KE_{COB} is stored so that only the person who knows KD_{COB} corresponding to KE_{COB} is authorized to write KE_{Cj}. These contents are written into the ROM 34 in the manufacturing process of the COB device 22 during the manufacture of the COB device before it is shipped to the mobile unit manufacturer. The contents are unalterable ... The EEPROM 36 can store personal information such as MSN, MSI, etc., a carrier public key KE_{Cj} 50 corresponding to a carrier secret key KD_{Cj} known only to the communications carrier, and a mobile unit public key KE_{MSNi} 52 corresponding to a mobile unit secret key KD_{MSNi} known only to the manufacturer of the mobile unit";

"wherein the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a new secret key Ki_2" is disclosed in '960 col. 7, lines 41-59 "The control program 40 includes programs for controlling input/output operations via the input/out terminal 38 as well as programs for encrypt/decrypt calculations expressed by equations (1) to (4), and all encrypt/decrypt operations in the mobile unit are performed within the COB device 22";

the following is not taught in '960: **"wherein the chip itself derives an initial secret key Ki_1"** however '086 teaches "Furthermore, the chip used in an embodiment of the present invention would have the ability to generate a public/private key pair for encryption and decryption of data and communications by the individual user. The cryptographic encryption keys may be of any acceptable asymmetric cryptographic type, such as RSA ... The private key so generated is then stored inside the chips in a non-readable and tamper-resistant manner. In addition, the chip would also have the ability, once a public/private encryption key pair for that device has already been generated, to rekey and generate a new public/private encryption key pair in place of the previous key pair" in col. 14, lines 66 through col. 15, line 17;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '960 a method of IC Card registration to include a means reuse IC cards with a new encryption key. One of ordinary skill in the art would have been motivated to perform such a modification because the ability to rekey the device will keep costs low and increase user popularity to use mobile devices (see '086 col. 8 lines 52 et seq.) "Unfortunately, there are many technical problems with the government's Clipper chip proposal, mostly stemming from the fact that the private keys to be escrowed are permanently embedded in the Clipper chips during manufacture. Because the private encryption key for a particular device is burned into the chip and cannot be changed, the chip and probably the entire device that contains it must be discarded if compromised. It is preferable for the user of a particular device to be able to rekey, reescrow and recertify the device at will if compromise is suspected or at regular intervals to avoid potential compromise ... If the concept of key escrow is to have significance,

each user must be able to choose his own trustees with whom to escrow his private keys, based upon the level of trust desired".

As to dependent claim 20, "wherein the chip includes means for receiving data from the security center (SC) and means for writing the received data to the memory" is taught in '960 col. 3, lines 49-63 "According to the present invention, there is also provided an IC card for an IC insertion type mobile unit for use in a mobile communications network, comprising: an input/output terminal; means for holding identification information used for connection to the mobile communications network; means for decrypting identification information and writing the same into the identification information holding means when an identification information write command, which contains the identification information, signature-encrypted with a secret carrier key of the communications carrier providing the mobile communications network, is entered via the input/output terminal; and means for reading out the identification information from the identification information holding means and outputting the same at the input/output terminal when an identification information readout command is entered via the input/output terminal, which command contains a mobile unit secret key of the manufacturer of the mobile unit for a model that can be used with the IC card inserted therein".

As to dependent claim 21, "wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC)" is shown in '960 col. 7, line 62 through col. 8, line 3 "The secret key KD and its corresponding public key are determined, e.g., in accordance with the RSA (Rivest-Shamir-Adleman) cryptosystem, but the present invention is not limited to this cipher system. It will be appreciated that the secret-key cryptosystem can also

be applied analogically. In the RSA cryptosystem, when the encrypt calculation for converting a plaintext M into a ciphertext C with the public key KE is expressed as".

As to dependent claim 22, "wherein the chip includes a dialing number which is fixedly programmed by the manufacturer" is disclosed in '960 col. 21, lines 4-11 "FIGS. 29 and 30 show the registration sequence for registering the IC card registration terminal with the communications carrier. Registration with any additional communications carrier is performed in the same sequence. In FIG. 29, first the COB device selector switch 176 (see FIGS. 23 and 24) is set to select the COB device holding the public key KE_{CN} of the desired carrier CN, and the telephone number of that carrier's terminal is dialed to request a connection".

As to dependent claim 26, "wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data to the security center (SC)" is taught in '086 col. 41, lines 17-26 "As previously described, the user also has the option of rekeying his device as to its user encryption key pair at any time after manufacture. The user does this by issuing a firmware instruction to the trusted device to perform the particular steps of the key escrow method, i.e. to generate a new private and public encryption key pair, send the key splits to the escrow agents and ultimately receive a new escrow certificate from the master escrow center".

7. **Claims 23-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over '960 in further view of '086 in further view in further view of Julin et al. U.S. Patent No. 5,557,679 (hereinafter '679).

As to dependent claim 23, the following is not taught in '960 and '086: **"wherein PIN and PUK default values are stored at the chip"** however '679 teaches "Each retailer has data

terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, 13 consisitng .... For generating IMSI, Ki, and PUK" in col. 3, lines 24-35.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of '960 and '086 a method of IC Card registration with a means to reuse IC cards to include a means to personalize an unblocking. One of ordinary skill in the art would have been motivated to perform such a modification because the personal unblocking key adds to the safety is an essential procedure see '679 (col. 1, lines 20 et seq.) "In mobile telephone systems, in which the mobile units are controlled by active cards assigned to the subscribers, the personalization of the respective card constitutes an essential procedure".

As to dependent claim 24, "wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated in the security center (SC) and transmitted to the chip" is disclosed in '679 col. 3, lines 24-35.

As to dependent claim 25, "wherein PIN and PUK default values are stored at the chip" is shown in '679 col. 3, lines 24-35.

8. **Claims 14-18,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '960 in further view of '086 in further view of Chatterjee et al. U.S. Patent No. 6,188,899 (hereinafter '899) in further view of Julin et al. U.S. Patent No. 5,557,679 (hereinafter '679).

As to independent claim 14, "A, method for personalizing GSM chips wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored, are stored, comprising the steps of:" is taught in '960 col. 7, line 40 through col. 8, line 67;

"a) performing the personalization of the chip when the subscriber logs on to the subscriber network for the first time" is disclosed in '960 col. 12, line 57 through col. 13, line 5 "FIG. 5 is a system setup diagram according to the present invention, for explaining the procedure for on-line registration of a mobile unit when a mobile unit purchased at a dealer authorized under contract with the communications carrier is registered via a registration terminal";

"b) obtaining the (ICCID) card number and the (IMSI) subscriber identification number from a number pool, is taught in '960 col. 7, line 40 through col. 8, line 67;

"the chip itself derives an initial secret; key Ki_1 from the. secret key Ki which is known and entered into the chip" is shown in '086 col. 14, lines 66 through col. 15, line 17;

"d) deriving at the authentication center (AC) the initial secret key Ki_1 ; e) setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center (SC) of the network operator; f) routing the connection from the chip to the security center (SC) during the first logon" is disclosed in '960 col. 21, line 19 through col. 22, line 7 "FIGS. 29 and 30 show the registration sequence for registering the IC card registration terminal with the communications carrier ... (see FIGS. 23 and 24) is set to select the COB device holding the public key KE_{CN} of the desired carrier CN, and the telephone number of that carrier's terminal is dialed to request a connection ... Upon receiving the random number RDM, the carrier's terminal signature-encrypts the received random number RDM with the carrier secret key KD_{CN}, and returns the result $E(KD_{CN}, RDM)$ (step e). Upon receiving $E(KD_{CN}, RDM)$, the IC card registration terminal sends the command of

item No. 11 in Table 2, containing the received E(KD_{CN}, RDM), the RDM stored in its RAM, and the integer J (J=1), to the internal COB (step f) to read out the carrier public key KE_{CN}";

"**g) negotiating between the chip and the security center (SC) a new second secret key Ki_2**" is shown in '086 col. 41, lines 17-26;

"**h) disabling the conditions of step e)**" is taught in '960 col. 9, lines 1-22 "The control program 54, fixed patterns 56, mobile unit secret key KD_{MSNi}, and mobile unit public key KE_{MSNi} are written during the manufacture of the mobile unit, while the flag 58 is caused to change state when the mobile unit is registered to the communications network" ;

the following is not taught in the combination of teachings of '960 and '086: "**c) making an entry in an authentication center (AC) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator**" however '899 teaches "FIG. 2 illustrates the over-the-air activation physical architecture. The mobile station 100 communicates over-the-air with the local base station 102, using the IS-136 standard. This standard is documented in TIA IS-136 Revision A, Mar. 21, 1996. The base station 102, the mobile switching center 104, and the visitor location register 106, are typically co-located at a local base station complex ... The over-the-air activation feature requires a notification be sent from the MSC 104 to the OTAF processor 110. This registration notification is via an IS-41 message on the Signaling System 7 (SS7) network. The fixed supporting network requires routing information to be able to send the registration notification from the MSC 104 to the proper network node, which in this case is the OTAF processor 110. In accordance with the invention, the mobile stations 100 are pre-programmed with information at the time of their manufacture to be able to request over-the-air activation. The unit of programmed information is

either the network routing address of the OTAF processor 110 or alternately it is a value that is translatable into that address. When the unactivated mobile station 100 powers up in the network, the mobile station requests activation over-the-air by transmitting to the local mobile switching center 104 a registration order that includes one of the three alternatives for pre-programmed information, either the routing address of the OTAF processor 110, or the OTAF ID number, or a dummy MIN value. The MSC 104 then forwards this information through the network to the over-the-air activation function processor 110" in col. 6, line 5 through col. 7, line 13;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '960 and '086 a method of IC Card registration with a means to reuse IC cards to include a means to send notification of activation of cards to a registration agent. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to send routing information to increase capabilities (see '899 col. 2 lines 31 et seq.) "Thus, there exists a need for a method and system to automatically route activation information sent over-the-air from the mobile wireless telephone set, through the fixed supporting network to an over-the-air activation processor in the network, where the activation parameters for the NAM module can be prepared and automatically downloaded over the network and sent over-the-air to the mobile wireless cellular telephone set";

the following is not taught in '960, '086, and '899 **"while PIN and PUK are set to a default value"** however '679 teaches "Each retailer has data terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, 13 consisitng .... For generating IMSI, Ki, and PUK" in col. 3, lines 24-35.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of '960, '086, and '899 a method of IC Card registration with a means to reuse IC cards to with a means to send notification of activation of cards to a registration agent to include a means to personalize an unblocking. One of ordinary skill in the art would have been motivated to perform such a modification because the personal unblocking key adds to the safety is an essential procedure see '679 (col. 1, lines 20 et seq.) "In mobile telephone systems, in which the mobile units are controlled by active cards assigned to the subscribers, the personalization of the respective card constitutes an essential procedure".

As to dependent claim 15, "wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established" is taught in '960 col. 8, lines 21-29.

As to independent claim 16, "further comprising the step of employing a Diffie Hellman method to negotiate the second secret key Ki_2" is taught in '086 col. 15, lines 2-20 "In another embodiment, Interactive Diffie-Hellman key generation can also be used, as discussed later, in order to ensure that all senders and recipients contribute new random numbers to generate the message session keys".

9. **Claims 17 and 18,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '960 in further view of '086, in further view of '899, in further view of '679, in further view of Brown et al. U.S. Patent No. 5,793,866 (hereinafter '866).

As to dependent claim 17, the following is not taught in '960, '086, '899, and '679: **"wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag)"** however '866 shows "The remote device 104 performs verification

functions ... However, if the intruder changes the modulus, the derived value received from the central site will not bear the predetermined relationship to the intruder's modulus, and the device will flag the insertion of the intruder's modulus and abort the activation process" col. 6 lines 45 through col. 7, line 4.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of '960, '086, '899 and '679 a method of IC Card registration with a means to reuse IC cards to with a means to send notification of activation of cards to a registration agent with a means to personalize an unblocking to include a means to flag the HLR. One of ordinary skill in the art would have been motivated to perform such a modification because an improved method to provide security protection is needed see '866 (col. 1, lines 64 et seq.) "Although the public key exchange is impervious to simple interception, it is vulnerable to a so-called "man –in the-middle" attack".

As to dependent claim 18, "wherein, when the initial secret key Ki_1 is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR)" is disclosed in '866 col. 4 lines 39-60 "The service provider, a central site, can also include a home location register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning. It has become desirable for over-the-air service provisioning to provide the subscription ID to the remote device 104, a mobile subscriber in the cellular system. This allows the subscription ID to be down-loaded from the central site 102, the service provider facility, to the subscriber remote device 104. In the OTASP protocol, a subscriber purchases a "blank" remote device, which is a remote device having no subscription ID. This remote device can originate a special purpose call to any of

several service providers (such as service provider central site 102) to request activation. With reference to FIG. 3, once the base station 202 recognizes the special-purpose call on the control channel, the potential subscriber is routed through a voice channel to the service provider to exchange OTA messages between the service provider central site 102 and the mobile subscriber remote device".

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
15 June 2005

David Y. Jung
Primary Examiner

6/24/05